Privacy and Confidentiality Policies and Procedures

Policy Rationale

1. Neighbourhood Support Waitakere hold a significant database that stores personal information about individuals and households in the community. It is important that those giving us their information can have trust and confidence that their information is safe and used for the purposes intended.

2. Our partnership and MoU with NZ Police means that Neighbourhood Support personnel are often privy to information and intelligence shared by Police. This information is provided on the understanding that we are trusted partners who will exercise discretion, respect confidentiality and comply with legal requirements and processes.

Policy Statement

1. All staff and volunteers of NS Waitakere who have access to NS databases and/or work within a Police premises will be Police Vetted, in accordance with our *Vetting and Code of Conduct Policy*.

2. All staff and volunteers of NS Waitakere will exercise good judgement and integrity when creating, accessing, modifying and using, securing and disclosing all information. We will handle information appropriately, for legitimate work purposes and in line with the law, our policies, processes and systems.

3. If a staff member or volunteer is unsure about whether information is confidential or sensitive or how it should be handled they should seek advice. This may include discussing the matter with their manager or Committee Chair, a Police Liaison Officer and/or NSNZ National Office.

4. NS Waitakere will make themselves familiar with the Protective Security Requirements as required by our MoU with NZ Police.

5. NS Waitakere will ensure that they understand and comply with the Official Information Act 1982 and the Privacy Act 2020.

6. NS Waitakere will comply with our Privacy and Confidentiality Procedures and Guidelines.

Date: 30 November 2020

Privacy and Confidentiality Procedures and Guidelines

Database Management

NS Waitakere will maintain an accurate and up-to-date database of Neighbourhood Support contacts.

1. When choosing a database or Client Management System (CMS) members should satisfy themselves that the platform is secure, verified and supported by a reputable software company.

2. Databases and CMS should be managed, maintained and accessed by only Neighbourhood Support personnel who have been Police Vetted and who have signed the NSNZ Code of Conduct.

3. Any database or CMS that stores personal information about individuals should be protected by security safeguards (such as passwords or encryption) that protect against it being accessed, used, modified or disclosed by unauthorised individuals or agencies.

4. Personal information held in databases and CMS should be protected against loss. Systems should be regularly backed-up and back-up copies should be securely stored, including cloud-based files.

5. If a database or CMS is linked to a website then the website should have the appropriate level of security and protection.

6. A Privacy Statement must be given to any individual who is entered into a NS database of CMS explaining why their information is being collected, who will have access to it and how it will be stored. A sample Privacy Statement is available in Appendix 1. A Privacy Statement can also be developed using the Privacy Commission's online tool: https://www.privacy.org.nz/tools/privacy-statement-generator/

7. Information shared by individuals and entered into a database or CMS should only be used for the purposes it was requested for (as outlined in the Privacy Statement.)

8. Personal information should not be kept for longer than is required for the purpose it was lawfully requested for and should be disposed of in a secure manner.

9. In the event that a member organisation discontinues its membership of NSNZ the database should be handed over to either the new member organisation in the area or NSNZ, who will maintain it until local arrangements can be made.

Newsletters, Alerts and Social Media

Neighbourhood Support Waitakere newsletters, alerts and social media messages frequently provide the community with information about crime prevention and safety. This may include sharing intelligence or information provided by NZ Police.

1. Reports of crimes shared in a NS newsletter should not identify the names or addresses of victims. General locations only should be used. The focus of newsletters should be on promoting prevention messages.

2. People suspected of a crime or suspicious behaviour should not be named or otherwise identified (including photos) in Neighbourhood Support newsletters, alerts or social media posts unless the Police have issued a specific warrant or notice, or otherwise verified and approved the information. To do so may put the organisation in breach of the Defamation Act 1992 and Principles 10 and 11 of the Privacy Act.

3. Photos of individuals, including children, should only be published with their permission and consent, or the consent of their parent or legal guardian (if they are under 18). Publishing photos of an identifiable individual without their consent (even if they are not named) can breach the Privacy Act.

Use of email

1. When sending out bulk emails the Blind Carbon Copy (BCC) function should be used so that individuals' email addresses are not published or circulated. Passing on email addresses without permission may breach the Privacy Act.

2. In general, it is not good practice to share confidential, personal or sensitive information via email because of the risk of error when entering the recipient's email address, the message being forwarded, or the email system being hacked. Good judgement, integrity and professionalism should be exercised when communicating by email.

3. All emails, including newsletters and bulk emails promoting Neighbourhood Support Waitakere, should comply with the Unsolicited Electronic Messages Act 2007. The following steps should be taken to avoid NS communications being considered spam:
    - Make sure that recipients have consented to receiving information from NS. This includes ensuring that NS members, or households who join NS, are aware that they will receive newsletters and information about our services when they join.
    - Emails should clearly identify the sender and include our logo and the sender's contact information.
    - Newsletters should have an Unsubscribe function or message so that people may opt out of receiving future emails if they choose.

Employment

The Privacy Act extends to personal information held about employees.

1. It is good practice to delegate the responsibility for managing employment matters to one or two people on a Committee (e.g. a Personnel Sub-Committee) or to the Manager. This provides a safe environment for the employee and reduces the chance for personal information about an employee being disclosed. If personal matters pertaining to an employee need to be discussed at a Committee or Board meeting, then this should be done In Committee and should not be included in publicly available minutes.

2. Personnel records should be stored securely and only accessed by those with delegated authority.

3. When an employee leaves their job their personnel records should not be held for any longer than legally necessary (e.g. for tax purposes), and should be destroyed in a secure manner (e.g. shredded).

4. Employees have the right to access the information held about them.

Related Legislation and Government Policies

Privacy Act 2020

At the heart of the Privacy Act are thirteen privacy principles. The privacy principles cover:

- collection of personal information (principles 1-4)
- storage and security of personal information (principle 5)
- requests for access to and correction of personal information (principles 6 and 7, plus parts 4 and 5 of the Act)
- accuracy of personal information (principle 8)
- retention of personal information (principle 9)
- use and disclosure of personal information (principles 10, 11, 12), and
- using unique identifiers (principle 13).

Under the Privacy Act 2020, if your organisation has a privacy breach that is likely to cause anyone serious harm, it is legally required to notify the Privacy Commission and any affected persons as soon as it is practicably able to.

For more information go to: https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

Further information can be found at:
https://privacy.org.nz/news-and-publications/guidance-resources/information-held-by-clubs-and-societies/

https://www.privacy.org.nz/tools/privacy-statement-generator/

Defamation Act 1992

Defamation is defined as damage to your reputation by unjustifiable attack. Under the Defamation Act, if someone wants to take an action for defamation they must establish a defamatory statement has been made, that that statement was about them and it was published by the respondent. Even if a statement implies or refers to a person, rather than specifically identifying them, a person can argue that they have been defamed.

Unsolicited Electronic Messages Act 2007

This Act protects people from receiving spam. Spam is the term for email, fax, text and image-based messages of a commercial nature that are sent to an individual without their having requested them. This includes the promotion of goods and services, even if they are free.

Further information can be found at: https://www.dia.govt.nz/Spam-Information-for-Businesses

Protective Security Requirements

The Protective Security Requirements (PSR) was passed by Cabinet in December 2014 due to government concerns around the quality and consistency of security within government agencies. It introduced 29 mandated security requirements under Governance, Personnel, Physical and information security. As a government agency NZ Police are required to comply with the PSR. Through NSNZ's Memorandum of Understanding with Police this extends to us. We have referred to the PSR when writing our policies and incorporated the relevant requirements.

Official Information Act 1982

The OIA is New Zealand's primary freedom of information law. The guiding principle of the Act is that information held by government agencies should be made available unless there is good reason for withholding it. Requests to Government Departments or State agencies for information must be answered "as soon as reasonably practicable", and within 20 working days.

Emails are subject to the OIA, which could mean that emails or communications between NZ Police and NSNZ or our member organisations could be subject to an OIA request.

Related NSNZ Policies

- NSNZ Vetting and Code of Conduct Policy
- NSNZ Child Protection Policy

Related NSNZ and Police Documents

- NSNZ Code of Conduct
- Police Code of Conduct